



DEPARTMENT OF THE ARMY
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX
75 6TH AVENUE
FORT KNOX, KENTUCKY 40121-5717

REPLY TO
ATTENTION OF:

Expires 16 August 2008

IMSE-KNX-IMO (25)

16 August 2006

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo No. 41-06 – Fort Knox Campus Area Network (FKCAN)
Connectivity Policy

1. References.

- a. Army Regulation 25-2, Information Assurance, 14 November 2003.
- b. Army Regulation 25-1, Army Knowledge Management and Information Technology, 15 July 2005.
- c. Department of Defense 5200.40, Information Technology Security Certification and Accreditation Process (DITSCAP).

2. Purpose. The purpose of this policy is to protect the FKCAN and its users from intentional or inadvertent security compromise. It establishes the rules for devices, sub-networks, and enclaves to obtain and maintain connection to the Fort Knox backbone and includes rules for hardware, software, and user performance. This policy dictates that the connected devices or sub-nets be accredited; be maintained and operated in accordance with the accreditation terms; and become part of the FKCAN. Therefore, they are subject to the Fort Knox Information Assurance Security staff monitoring and enforcement. Adherence to this policy will reduce the risk of alteration, theft, or destruction of data and denial of service.

3. Applicability. The FKCAN connectivity policy applies to all subscribers that have access to the FKCAN and all devices connected to it.

4. Overview. Network connection rules must be consistent with network accreditation criteria. Accreditation is the culmination of a strict procedure that organizes and configures automated information systems (AISs) to achieve an acceptable level of risk of exploitation. Networks must be accredited before they can be made operational. A designated approving authority (DAA) grants this accreditation, and any changes to the network that affect security must be approved by the DAA before implementation. All connected devices, local area networks (LANs) and enclaves, regardless of the command affiliation of their owner, must adhere to a single connection rule policy. The DOIM is mandated by reference 1a to verify compliance with this policy and imposes restrictions on connected systems for noncompliance.

5. Accreditation. Units requesting connection of a device, LAN (including connections to quarters), or enclave to the FKCAN, must provide the Fort Knox DAA a complete description of the device, network or enclave, and accreditation documents. After connection is authorized, any updates or changes to the tenant network will be provided to the installation information assurance manager (IAM) for approval before implementation. The Fort Knox IAM will determine if the new or changed system complies with the FKCAN accreditation and, if not, require the requesting agency to make the system compliant. The Fort Knox DAA will determine if connecting the systems will result in the need to reaccredit either or both systems.

6. Memorandum of Agreement (MOA). The requesting unit's DOIM or information assurance (IA) personnel and the Fort Knox DOIM will develop an MOA that establishes the operating conditions that must be maintained by both parties. The MOA will describe all of the conditions necessary to maintain an optimum, secure, non-interfering connection that conforms to the FKCAN accreditation. The MOA will stipulate that any changes in the requesting unit's system that affects system integrity or security will require Fort Knox DAA approval before implementation. Connection to the installation backbone constitutes consent to announced and unannounced verification of security features including automated vulnerability scanning, modem identification scanning, and physical inspection. Failure to comply with the FKCAN policies, ARs, and/or DOD memorandums may result in disconnection from the network infrastructure. Exceptions to policy must be requested, in writing, to the Director, Information Management.

7. Roles and Responsibilities.

a. Designated Approving Authority (DAA). The Fort Knox Garrison Commander is the FKCAN DAA and is responsible for ensuring the FKCAN is compliant with the system certification stipulations. The Fort Knox DAA decides if IA measures taken have mitigated security risks to the FKCAN sufficient to warrant operation on the network.

b. Information Assurance Manager (IAM). The installation IAM enforces adherence to the accreditation terms and can require tenants to provide special equipment necessary to support the tenant requirements for network connection. The installation IAM is authorized to verify security features by automated vulnerability scanning, modem identification scanning, and physical inspection to check for compliance with the FKCAN connectivity policy. The installation IAM is authorized to disconnect or limit the connection of devices, LANs, and enclaves that fail to meet terms of the accreditation or the MOA.

8. Connection Procedures.

a. Any activity (Fort Knox or tenant) wishing to connect a network system to the Fort Knox backbone will, prior to connection, provide a description (pictorial and narrative) of the

IMSE-KNX-IMO (25)

SUBJECT: Fort Knox Policy Memo No. 41-06 – Fort Knox Campus Area Network (FKCAN)
Connectivity Policy

network/system being connected. This description will show the IP addresses assigned to each bridge, router, and/or switch connected to the network and all external connections and their locations. Additionally, the description should strive to associate IP sub networks to physical segments for the switches, and so forth. Any system updates or changes to the network will be submitted for approval and incorporation into the installation site C & A.


b. Tenant activities and proponents for fielded systems (DA or DOD) will comply with the installation IA policy and may request further information assurance oversight or assistance. In addition to requirement in 8a above, a copy of the system accreditation package will be provided. The package will include the following:

- (1) Certification evaluation, report of findings, and statement.
- (2) Security Risk Management Review.
- (3) System Security Authorization Agreement.
- (4) Security Test & Evaluation Plan.
- (5) Accreditation Statement.

c. All documentation will be reviewed by the installation IAM and security implications to the installation backbone identified prior to receiving an approval to connect.

9. Point of contact for additional information is the installation IAM, phone DSN 464-7201.

FOR THE COMMANDER:


MARK D. NEEDHAM
COL, AR
Garrison Commander

DISTRIBUTION:

C

CF:

Commanders, Fort Knox Partners in Excellence